

X. Zheng ¹ ¹ PhD Student, School of Law of Wuhan University
(Wuhan, People's Republic of China)

ORCID ID: 0009-0003-3560-6694, e-mail: zxx577374942@gmail.com

THE RESTRICTED APPLICATION OF THE CRIME OF “INFRINGEMENT OF CITIZENS' PERSONAL INFORMATION” IN CHINESE CRIMINAL LAW

Abstract. This article explores the narrow application of the crime of infringing citizens' personal information under the reverse connection of criminal and administrative law enforcement by analyzing its judicial expansion obstacles, clarifying relevant theoretical and institutional foundations, and proposing three targeted regulatory solutions. In current Chinese criminal law, the judicial application of the crime of infringing upon citizens' personal information keeps expanding, giving rise to prominent problems including inconsistent administrative and criminal sanctions for identical cases as well as conflicting normative criteria between criminal and administrative laws. Article 56 of the revised Public Security Administration Punishment Law of 2025 provides a normative foundation for reverse administrative-criminal connection and the restrictive application of this crime. Based on the “quantitative difference theory” to distinguish administrative illegality from criminal illegality and combined with the prudent punishment philosophy in the misdemeanor era, this paper sorts out three major obstacles hindering the reverse administrative-criminal connection of the crime: fragmented normative definitions, disconnection between administrative-criminal sanctions in practice, and the inertia of criminal priority squeezing the space for exoneration. Relying on the theoretical and institutional basis of reverse administrative-criminal connection, this paper proposes three approaches: unifying the definition and grading criteria of “personal information”, substantively identifying the standard of “serious circumstances”, and strictly narrowing the interpretation of “violating relevant state provisions”.

Key words: administrative-criminal connection, personal information protection, quantitative difference theory, crime of infringing upon citizens' personal information.

Introduction

In recent years, the crime of infringing on citizens' personal information has been rampant in Chinese judicial practice. According to data released by the Supreme People's Procuratorate, in the past five years, procuratorial organs nationwide have prosecuted an average of over 7,000 individuals annually for this crime. In 2024 alone, procuratorial organs nationwide prosecuted 2,458 individuals for crimes involving the use of the internet to infringe on citizens' personal information ¹. Furthermore, a search on the “Peking University Legal Database” case

platform using “crime of infringing on citizens' personal information” as a keyword yielded 14,627 criminal cases as of May 2026 ². The distribution by year shows a surge in cases starting in 2017, and the number has remained high since then, reflecting the expansion of this crime's application in the judiciary. Historically, the legal protection of personal information has been characterized by a “criminal law first” approach. Although the promulgation of laws such as the Cybersecurity Law and the Personal Information Protection Law has stipulated administrative penalties for acts of infringing on citizens' personal information, thus restoring the

¹ Supreme People's Procuratorate of China. Prosecutors indicted 2,458 persons for crimes of infringing citizens' personal information committed via the internet in 2024. URL:

https://www.spp.gov.cn/spp/2025zgjjzbg/202503/t20250308_688216.shtml (accessed: 30.05.2026).

² All Case Data Comes from the Peking University Legal Database Website. URL: <https://www.pkulaw.com> (accessed: 30.05.2026).



Criminal Law to a “secondary law” role, it has not effectively alleviated the current situation of judicial expansion. On the one hand, the judicial expansion of the crime of infringing on citizens' personal information reflects the active efforts of judicial organs in the era of big data to combat crimes involving the infringement of citizens' personal information through the internet and protect citizens' information security. On the other hand, the “overheating” of the judiciary has brought new challenges to the standardized protection of personal information. For example, the excessive application of criminal law can easily lead to problems such as infringement of citizens' freedom and waste of judicial resources. Therefore, how to achieve effective connection between criminal law and relevant prior laws, and thus limit the application of the crime of infringing on citizens' personal information, has become the focus of research on this crime.

Currently, Chinese courts exhibit a mismatch between the sentencing discretion in cases of infringing on citizens' personal information and the penalties stipulated by law. Some scholars have pointed out that courts clearly impose lenient sentences for this crime, and that more than half of the cases result in suspended sentences [1]. The phenomenon of lenient sentencing in judicial practice reflects a deviation from the actual sentencing for this crime, while also providing practical space for the narrowing application of this crime and the intervention of administrative penalties.

In June 2025, the revision of the Public Security Administration Punishment Law ³ provided a legal opportunity for the connection between administrative and criminal penalties in personal information protection. Article 56 stipulates that “anyone who violates relevant national regulations by selling or providing personal information to others shall be detained for not less than ten days but not more than fifteen days; if the circumstances are minor, he shall be detained for not more than five days. Anyone who steals or illegally obtains personal information by other means shall be punished in accordance with the provisions of the preceding paragraph”. This provision is highly similar to the provisions of Article 253-1 of the Criminal Law ⁴ concerning

the crime of infringing on citizens' personal information, making the tiered legal protection of citizens' personal information more complete, and providing a normative basis for the criminal exclusion of this crime and the reverse connection between administrative and criminal penalties.

Clearly, the revision of the Public Security Administration Punishment Law is a response to the current phenomenon of judicial expansion. However, with the improvement of the legal system for personal information protection, how to reasonably define the boundaries between administrative and criminal penalties in personal information protection and avoid the phenomenon of applying different laws to the same case has become an urgent problem to be solved.

Materials and Methods

This study employs a research methodology combining literature analysis with comparative research.

First, through a literature review, it identifies excessive judicial expansion of the crime of infringing citizens' personal information and three practical obstacles. Second, it compares illegality differentiation theories and adopts the quantitative difference theory, illustrating theoretical and institutional foundations from prudent punishment thought and the 2025 revised Public Security Administration Punishment Law. Third, it contrasts conflicting judicial cases to prove blurred criminal-administrative boundaries. Finally, it proposes three restriction paths: unified personal information standards, substantive judgment of “serious circumstances”, and strict interpretation of national provisions. Data sources include international legal documents, national data protection rules, open journals and books.

Results and Discussion

1. Practical Obstacles to the Restricted Application of the Crime of Infringing on Citizens' Personal Information

In the field of personal information protection, with the continuous improvement of relevant prepositive legal norms, a multi-layered legal protection framework covering civil,

³ Public Security Administration Punishments Law. URL: https://www.pkulaw.com/en_chl/4a0675f698316d0fbdbf.html (accessed: 30.05.2026).

⁴ Criminal Law of the People's Republic of China. URL: https://www.pkulaw.com/en_chl/3b70bb09d2971662bdfb.html (accessed: 30.05.2026).



administrative and criminal laws has now taken shape, and the model of “prior criminal intervention” has long come to an end. Nevertheless, the reverse connection mechanism between administrative law enforcement and criminal justice remains inefficient in judicial practice, which creates obstacles to restricting the overexpansive application of the crime of infringing upon citizens' personal information.

1.1 Fragmented Legal Provisions Lead to a Lack of Linkage Standards

Currently, the specific application rules for the crime of infringing on citizens' personal information in China's Criminal Law are mainly stipulated by the “Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing on Citizens' Personal Information” jointly promulgated by the Supreme People's Court and the Supreme People's Procuratorate in 2017, providing the core basis for conviction and sentencing in judicial practice. The preceding laws linking this crime mainly include the Civil Code, the Personal Information Protection Law, the Cybersecurity Law, and the Public Security Administration Punishment Law. While a comprehensive legal system provides a normative basis for the comprehensive governance of acts infringing on citizens' personal information, the blurred boundaries and overlapping concepts between substantive legal norms have failed to form a systematic and hierarchical legal normative system, becoming an obstacle to the linkage between administrative and criminal law in personal information protection.

Firstly, the Judicial Interpretation on Criminal Cases Involving Personal Information is inconsistent with other prior legal regulations regarding the scope of “personal information”. The Judicial Interpretation ⁵ defines “personal information” as: “various information recorded electronically or otherwise that can, alone or in combination with other information, identify a specific natural person or reflect the activities of a specific natural person”. Article 1034 of the Civil Code ⁶ defines “personal information” as:

“various information recorded electronically or otherwise that can, alone or in combination with other information, identify a specific natural person”. Article 4 of the Personal Information Protection Law ⁷ defines personal information as: “various information recorded electronically or otherwise that relates to an identified or identifiable natural person”. Thus, the Civil Code and the Personal Information Protection Law are essentially consistent in their definition of “personal information”, limiting the object to “various information about natural persons”. However, the Judicial Interpretation on Criminal Cases Involving Personal Information includes “various information reflecting the activities of a specific natural person” within the scope of personal information protection, clearly indicating that this interpretation's scope of personal information is broader than that stipulated by the prior laws [2]. According to the principle of the unity of legal order, the evaluation of the same behavior in different legal fields needs to be consistent. Criminal law needs to maintain restraint; for behaviors permitted by other laws, criminal law should not deem them crimes. However, the Judicial Interpretation on Criminal Cases Involving Personal Information improperly expands the scope of “personal information”, clearly violating this principle.

Secondly, the classification standards for “personal information” in the Judicial Interpretation on Criminal Cases Involving Personal Information differ from the provisions of the preceding law. Article 5 of the Judicial Interpretation on Criminal Cases Involving Personal Information divides “personal information” into three categories based on the importance of the information: sensitive information, important information, and general information. For sensitive information, a conviction is warranted if the number of illegally obtained, sold, or provided exceeds 50 pieces; for general information, it requires more than 5,000 pieces. However, Chapter 2 of the Personal Information Protection Law divides “personal information” into general personal information

⁵ Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing on Citizens' Personal Information. URL: https://www.pkulaw.com/en_chl/88d3a698daf58033bdfb.html (accessed: 30.05.2026).

⁶ Civil Code of the People's Republic of China. URL: https://www.pkulaw.com/en_chl/aa00daaeb5a4fe4ebdfb.html (accessed: 30.05.2026).

⁷ Personal Information Protection Law of the People's Republic of China. URL: https://www.pkulaw.com/en_chl/d653ed619d0961c0bdfb.html (accessed: 30.05.2026).



and sensitive personal information, applying different protection rules to different levels of personal information. The different provisions regarding the classification of “personal information” in the Judicial Interpretation on Criminal Cases Involving Personal Information and the Personal Information Protection Law lead to overlap and ambiguity in the identification standards among various types of information [3]. For example, the Personal Information Protection Law defines sensitive personal information as: “personal information that is likely to infringe upon the personal dignity of natural persons or endanger their personal or property safety, including biometrics, religious beliefs, specific identities, medical and health information, financial accounts, and location tracking information”. The “biometrics”, “location tracking”, and “medical and health information” listed in this provision can be respectively correlated with sensitive information and important information in the Judicial Interpretation on Criminal Cases Involving Personal Information [4]. This has led to two different classification standards for certain sensitive personal information when applying the crime of infringing on citizens' personal information. The difference between the two classification standards directly affects the criteria for judging “serious circumstances”, which can easily lead to disputes over the application of administrative penalties and criminal penalties in practice.

1.2 Practical Deficiency in the Connection Between Administrative and Criminal Law

Traditionally, Article 253-1 of China's Criminal Law stipulates criminal penalties for serious violations of citizens' personal information, while administrative penalties are mainly stipulated by Article 66 of the Personal Information Protection Law and Article 64 of the Cybersecurity Law⁸ for those that do not meet the standards for a crime. However, for a long time, the failure to fully communicate the relationship

between criminal law and administrative penalties in personal information protection has led to the phenomenon of “different judgments for the same case” in judicial practice. For example, in the “Didi's exorbitant fine case”⁹, Didi's illegal and excessive collection of massive amounts of personal information clearly met the constituent elements of the crime of infringing on citizens' personal information. However, the final outcome of this case was only to impose administrative penalties through the application of laws such as the Personal Information Protection Law, excluding the application of the Criminal Law. In the case of Xie's infringement of consumer personal information [5], Xie's illegal collection of more than 20,000 pieces of consumer personal information was also only subject to administrative penalties under Article 56 of the Consumer Rights Protection Law¹⁰. In contrast, in the case of Ke¹¹, who was charged with infringing on citizens' personal information and whose case was similar in nature, Ke was criminally punished, reflecting the conflation of criminal and administrative penalties in practice [6].

Furthermore, the determination of illegally obtaining publicly available personal information has led to inconsistent judgments in judicial practice due to the application of different legal standards by judicial personnel. For example, in the case of Wu selling business registration information [7], the public security organs summoned Wu on suspicion of infringing on citizens' personal information for downloading and selling more than 18,000 pieces of business registration information from websites such as Tianyancha and Qichacha. After review by the procuratorate, it was determined that Wu's actions did not constitute illegal processing of personal information according to Article 1036 of the Civil Code, and therefore did not constitute the crime. However, in the case of Li et al. infringing on citizens' personal information¹², the court, based on the “Judicial Interpretation on Criminal Cases

⁸ Cybersecurity Law of the People's Republic of China. URL: https://www.pkulaw.com/en_chl/fe9682732480b562bdfb.html (accessed: 30.05.2026).

⁹ Didi Fined 8.026 Billion Yuan for 16 Illegal Acts. URL: https://www.zjwx.gov.cn/art/2022/7/21/art_1673576_58871621.html (accessed: 30.05.2026).

¹⁰ Law of the People's Republic of China on the Protection of Consumers' Rights and Interests. URL:

https://www.pkulaw.com/en_chl/a347c82e6a7d13aabdfb.html (accessed: 30.05.2026).

¹¹ Case of Ke Illegally Infringing upon Citizens' Personal Information. URL: <https://www.pkulaw.com/pfnl/95b2ca8d4055fce158471146f021a62ebf0dbf078e8cb38bdfb.html> (accessed: 30.05.2026).

¹² Second Instance Criminal Ruling on the Crime of Infringing upon Citizens' Personal Information Involving Li Z, Wang C and Others. URL:



Involving Personal Information”, treated credit information containing publicly available personal information as sensitive information, and therefore determined it to be the crime of infringing on citizens' personal information. The different determinations in the aforementioned cases reflect the different conclusions reached by judicial personnel due to the application of different laws.

1.3 Criminal Expansion Squeezes and Limits Application Space

For a considerable period after the Ninth Amendment to the Criminal Law in 2015 added the crime of infringing on citizens' personal information, administrative protection of personal information remained absent. During this period, criminal penalties encompassed all means of personal information protection, resulting in a phenomenon of “criminal law taking precedence”. Although the promulgation of the Cybersecurity Law, the Personal Information Protection Law, and the Civil Code has relegated the application of the Criminal Law to a secondary role in terms of regulations, the long-standing inertia of prioritizing criminal penalties has not been broken.

As the most severe means of social sanctions, criminal penalties must adhere to the principle of “restraint”. Criminal law should only intervene as a last resort when other branches of law, such as civil law and administrative law, are insufficient to fully protect a certain social relationship. This legal logic also applies to the field of personal information protection. Therefore, the correct logic for protecting personal information should begin with prior laws; criminal penalties should only be applied when administrative penalties are insufficient to protect personal information. However, in practice, this logic is precisely the opposite. In the protection of personal information, the lack of prior legal buffers, stemming from the precedence of criminal and administrative sanctions, easily leads judicial personnel to prioritize Article 253-1 of the Criminal Law when handling cases. Specifically, when faced with new types of cases involving the infringement of citizens' personal information, judicial personnel only consider whether the infringed “personal information”

meets the requirements of Article 1 of the Judicial Interpretation on Criminal Cases Involving Personal Information and whether the “serious circumstances” meet the requirements of Article 5 of the Judicial Interpretation on Criminal Cases Involving Personal Information, while ignoring the provisions of prior laws such as the Personal Information Protection Law and the Civil Code regarding the infringement of citizens' personal information. This practice is highly likely to lead to the expansion of criminal penalties in personal information cases.

2. Theoretical Basis and Institutional Basis for the Reverse Connection Between Administrative and Criminal Law in Cases of Infringement of Citizens' Personal Information

To limit the application of the crime of infringing upon citizens' personal information, it is necessary to start with the reverse connection between administrative and criminal law in personal information protection. The reverse connection between administrative and criminal law consists of two parts: “exclusion from criminal liability” and “entry into criminal law”. Therefore, it is essential to clarify the boundary between administrative and criminal offenses to establish a tiered legal protection system for personal information. Secondly, in the context of governing minor offenses, it is necessary to implement the principle of restraint and caution in sentencing, using criminal law measures prudently, and properly handling the relationship between the Public Security Administration Punishment Law, the Personal Information Protection Law, and the Criminal Law.

2.1 Distinction Between Administrative and Criminal Law: The Theoretical Basis for the Reverse Connection Between Administrative and Criminal Law

2.1.1 The Logic of the Distinction Between Administrative and Criminal Offenses

The relationship between administrative and criminal offenses has been discussed for a long time in the field of criminal law. Currently, three different viewpoints have been formed: the “qualitative difference theory”, the “quantitative difference theory”, and the “quality distinction theory”. Among them, the “qualitative difference theory” emphasizes that administrative and



criminal offenses differ in nature, therefore their quantities cannot be compared. The first argument is based on the premise that criminal law aims to protect legal interests, while administrative law aims to maintain order; their natures differ, necessitating a distinction. "Criminal wrongdoing is specifically determined by morally worthless evaluation, while administrative wrongdoing is limited to simple disobedience to administrative orders" [8]. The "quantitative difference theory" argues that administrative wrongdoing and criminal wrongdoing are not different in nature, but only differ in the degree of illegality. Its basis is that illegality refers to a violation of the overall legal order, a commonality in both criminal and administrative law. "Criminal law does not create a new legal order, but merely confirms the existing one" [9]. As a safeguarding law, criminal law cannot independently create prohibitive norms; it must rely on norms established by other preceding legal fields such as civil law and administrative law. Therefore, administrative wrongdoing and criminal wrongdoing can be distinguished by differences in "quantity". The "qualitative difference theory" argues that administrative wrongdoing and criminal wrongdoing have qualitative differences in core areas, while quantitative differences exist in non-core areas [10]. This theory does not adopt a single standard for distinguishing wrongdoing but rather represents a compromise between the first two viewpoints.

This article argues that the aforementioned theoretical debates are essentially interpretations chosen by different scholars based on different academic perspectives and research methods. There is no absolute right or wrong; what needs to be considered is which theory aligns with the legislative and judicial realities of the country. Therefore, based on Chinese practice, this article argues that the "quantitative difference theory" has merit for the following reasons:

First, the "quantitative difference theory" aligns with Chinese substantive law. Under China's "dual sanctions system", administrative and criminal offenses overlap significantly. For the same behavior, both criminal and administrative penalties are often stipulated simultaneously, and the wording of these provisions is similar. Specifically, the Criminal Law contains many expressions of "serious circumstances", meaning that only when a

behavior reaches the level of "serious circumstances" can it be punished under criminal law; for behaviors that do not reach this level, administrative measures are used. The "qualitative difference theory", which argues for a difference in nature between administrative and criminal penalties, is out of touch with Chinese legislation.

Second, the "quantitative difference theory" offers clearer distinctions and is more practically feasible. The "qualitative difference theory" argues that criminal offenses involve the infringement of legally protected interests under criminal law, which is the core distinction between criminal and administrative offenses. However, legally protected interests are an abstract concept, especially in the realm of administrative crimes, making it impractical to define the boundary between administrative and criminal offenses based solely on the concept of legally protected interests. The "quantitative difference theory", on the other hand, seeks to differentiate based on the degree of illegality, which is commonly expressed in Chinese jurisprudence as "serious circumstances". For example, Article 253-1 of China's Criminal Law requires "serious circumstances" to establish the crime of infringing on citizens' personal information, while Article 56 of the Public Security Administration Punishment Law stipulates penalties for general circumstances and less serious circumstances. This quantitative distinction is clearly more explicit.

Finally, the "quantitative difference theory" aligns inherently with the mechanism for linking administrative and criminal law. Due to the extensive overlap between administrative and criminal offenses in China, many laws directly stipulate provisions for linking administrative and criminal law. For example, Article 71 of the Personal Information Protection Law stipulates: "Anyone who violates the provisions of this Law and whose conduct constitutes a violation of public security administration shall be punished according to law; if the conduct constitutes a crime, criminal liability shall be pursued according to law". The premise of administrative and criminal law linkage lies in the existence of the same illegal act. If the "qualitative difference theory" is taken to its extreme, denying the homogeneity between administrative and criminal illegality, then there is no room for



administrative and criminal law linkage. Therefore, only by adopting the “quantitative difference theory” can the linkage between administrative and criminal law be reasonably explained.

2.1.2 The Development of Cautious Punishment in the Era of Minor Offenses

Recent crime statistics indicate that China has entered an era of minor offenses. Firstly, a structural shift has occurred in the types of crimes in China. In recent years, over 80% of criminal cases in China have resulted in sentences of three years or less imprisonment, while the proportion of serious crimes continues to decline.¹³ Secondly, the scope of the Criminal Law is expanding. New crimes and new forms of conduct have been continuously added through amendments to the Criminal Law in recent years. These new crimes and conduct largely reflect current social governance needs, and the statutory penalties are mostly minor offenses with sentences of three years or less imprisonment. Thirdly, China's social governance philosophy has shifted from “punishing crime” to “governance”, emphasizing crime prevention and diversified governance. In current judicial practice, China has abandoned the past ideology of “severe crackdown” and “heavy punishment”, emphasizing a criminal policy of “combining leniency with severity” and the idea of “cautious punishment”. The application of lenient penalties in judicial cases is gradually becoming a trend. As mentioned earlier, in cases of crimes involving the infringement of citizens' personal information, the actual penalties imposed by judicial organs are far lower than the statutory penalties, and probation is applied to defendants in a large number of cases.

The concept of cautious punishment originated from the “enlightened virtue and cautious punishment” in the Western Zhou Dynasty of ancient China, and gradually became the mainstream legal thought in ancient Chinese society. Many of its connotations remain significant in today's society. As General Secretary Xi Jinping pointed out: “The Chinese

legal system embodies the spirit and wisdom of the Chinese nation, and many excellent ideas and concepts are worth inheriting... The concept of cautious punishment with virtue as the primary principle and punishment as the secondary principle... etc., all demonstrate the wisdom of the excellent legal culture of the Chinese nation”¹⁴. At the level of criminal law philosophy, the “considerate punishment” concept emphasizes “virtue as the primary principle and punishment as the secondary principle”, that is, social governance should be based on virtue, with punishment as a supplementary means. The purpose of punishment is not to punish, but to serve social governance. The “collaborative governance” inherent in the concept of cautious punishment advocates that criminal law should work together with other means, each playing its role appropriately [11]. This aligns with the diversified treatment model advocated in the current governance of minor crimes in China. In terms of sentencing, the “prudent approach to punishment” advocates for “lighter penalties in times of peace and harsher penalties in times of chaos”. The current “combination of leniency and severity” criminal policy advocated in China is a concrete manifestation of this traditional prudent approach to punishment in the contemporary judicial field. Entering an era of minor offenses, the in-depth implementation of this prudent approach in judicial practice provides a solid ideological foundation and theoretical support for the construction and operation of the current reverse linkage mechanism between punishment and sentencing.

2.2 Institutional Basis for the Reverse Linkage Between Administrative and Criminal Law in Personal Information Protection

The reverse linkage between administrative and criminal law is not a product of chance, but rather rooted in China's local realities and legislative environment. As an important avenue for acquitting minor offenses, it reflects China's current criminal policy of “combining leniency with severity” and its cautious approach to punishment. Furthermore, the 2025 revision of the

¹³ Vice President Yang Wanming of the Supreme People's Court: Applying the Leniency System for Admission of Guilt and Acceptance of Punishment and Promoting the Modernization of Misdemeanor Trials. URL: <https://www.court.gov.cn/zixun/xiangqing/427612.html> (accessed: 30.05.2026).

¹⁴ Unswervingly Follow the Path of Socialist Rule of Law with Chinese Characteristics to Provide Strong Legal Safeguards for Building a Modern Socialist Country in All Respects. URL: https://www.qstheory.cn/dukan/qs/2021-02/28/c_1127146541.htm (accessed: 30.05.2026).



Public Security Administration Punishment Law provides an institutional basis for this linkage, with Article 56 of the law holding unique institutional value.

As mentioned earlier, the newly revised Public Security Administration Punishment Law stipulates administrative penalties for acts that infringe upon citizens' personal information, addressing the previous inadequacy in administrative protection of personal information. Prior to this, although Article 71 of the Personal Information Protection Law stipulated that “any violation of this Law constituting a violation of public security administration shall be punished according to law based on public security administration”, there were no relevant provisions for such penalties at the time, rendering the article ineffective. Traditionally, legal liability for infringing on citizens' personal information typically involves imposing fines under prior laws such as the Personal Information Protection Law and the Civil Code. For serious offenses, Article 253-1 of the Criminal Law is directly applied, imposing imprisonment and fines. This approach lacks a proper buffer between administrative and criminal penalties, blurring the lines between the two and potentially leading to undue expansion of criminal law.

However, after the revision of the Public Security Administration Punishment Law, for acts infringing on citizens' personal information, Article 141 can be applied directly. For offenses not reaching the level of a crime, both Article 66 of the Personal Information Protection Law (administrative penalties) and Article 56 of the Public Security Administration Punishment Law (administrative detention) can be applied. For serious offenses, criminal law can be used directly. Furthermore, the revised Article 56 of the Public Security Administration Punishment Law and Article 253-1 of the Criminal Law are highly similar in content, eliminating practical obstacles to the application of these provisions. Therefore, the revision of the Public Security Administration Punishment Law is of great significance for alleviating the current excessive expansion of crimes involving the infringement of citizens' personal information and improving the reverse linkage mechanism between administrative and criminal penalties for personal information protection.

3. Paths for Restricting the Application of

the Crime of Infringing Citizens' Personal Information Under Reverse Administrative Criminal Connection

For a long time, the root cause of the judicial expansion of the crime of infringing on citizens' personal information lies in the ambiguity of the boundaries between administrative and criminal law, leading to its mixed application in judicial practice. Therefore, to achieve judicial restriction of the crime of infringing on citizens' personal information, it is necessary to establish a hierarchical protection system for personal information and form a multi-faceted and collaborative governance model involving civil, administrative, and criminal law based on the “quantitative difference theory”.

3.1 Unifying the Standards for Identifying “Personal Information”

As mentioned above, the different understandings of “personal information” between criminal law and prior laws have led to the inappropriate expansion of the scope of “personal information” in judicial practice, thus hindering the realization of the reverse connection between administrative and criminal law in personal information protection. Therefore, it is necessary to unify the understanding of “personal information” as stipulated in positive law. According to the “quantitative difference theory”, the judgment of illegality should be based on a holistic evaluation. Criminal law should be subordinate to the norms of prior laws and cannot create illegality independent of civil and administrative law. Therefore, the scope of “personal information” in criminal law must be in accordance with the provisions on “personal information” in the Personal Information Protection Law and the Civil Code. Specifically, the Judicial Interpretation on Criminal Cases Involving Personal Information defines “personal information” as “various information concerning the identity of a specific natural person or reflecting the activities of a specific natural person”, a scope broader than the “various information about a natural person” stipulated in the preceding law. Therefore, the scope of “personal information” in the Judicial Interpretation on Criminal Cases Involving Personal Information should be adjusted to align with the preceding law. Furthermore, the classification standards for “personal information” differ between the Judicial



Interpretation on Criminal Cases Involving Personal Information and the Personal Information Protection Law; these classification standards should be unified to avoid confusion in judicial application.

3.2 Substantive Standards for Determining “Serious Circumstances”

Currently, the standards for criminalizing the crime of infringing on citizens' personal information and the statutory standards for escalating penalties are mainly based on Article 5 of the “Judicial Interpretation on Criminal Cases Involving Personal Information”, namely, a “tiered + quantitative” model. For sensitive information, more than 50 infringing items constitute a serious offense; for important information, the number needs to reach 500; and for general information, it needs to reach 5,000. This quantitative standard is easy to distinguish and highly operable in practice, but it is prone to falling into the trap of “quantity over quality”, leading to a formalistic standard for criminalization. In the era of big data, perpetrators illegally obtain citizens' personal information in the tens of thousands through the internet. Not all acts of infringing on citizens' personal information deserve criminal protection; otherwise, it would lead to an overly “bloated” criminal law. Therefore, this article suggests that the standard for determining “serious circumstances” should be based on a substantive judgment of the harmfulness of the act. Building upon the existing standards for criminalization, it should focus on examining the methods of illegally obtaining personal information and the actual damage caused to legal interests, thereby limiting the criminalization of such acts.

3.3 Strict Interpretation of “Violation of Relevant National Regulations”

As a statutory offense, the crime of infringing upon citizens' personal information must be established on the premise that the act “violates relevant national regulations”. However, the “Judicial Interpretation on Criminal Cases Involving Personal Information”, in order to meet the practical needs of punishing crime, includes “departmental regulations” within the scope of “relevant national regulations”. This undoubtedly unduly expands the scope of

“relevant national regulations” and is suspected of violating the principle of legality in criminal law. Therefore, “violation of relevant national regulations” must be strictly interpreted. First, acts that only formally violate relevant national regulations without substantively contradicting the spirit behind the regulations and thus infringing upon others' personal information rights cannot be considered “violations of relevant national regulations”. Second, the scope of “departmental regulations” is too broad and difficult to define. Therefore, “departmental regulations” should be excluded from “relevant national regulations”. The application of the crime of infringing upon citizens' personal information should only be premised on “violation of laws and administrative regulations concerning the protection of citizens' personal information”, to avoid an excessively broad scope of criminal punishment and unduly infringing upon citizens' freedom.

Conclusion

This study identifies the widespread overexpansion of the crime of infringing citizens' personal information in judicial practice, stemming from fragmented legal definitions, disjointed criminal-administrative coordination and long-standing criminal priority inertia. Adopting the quantitative difference theory and prudent punishment doctrine, the paper takes the 2025 revised Public Security Administration Punishment Law as the institutional basis for reverse criminal-administrative linkage. To realize restrained application of this crime, three targeted measures are proposed: unifying the definition and classification standards of personal information consistent with prepositive laws, substantively judging “serious circumstances” instead of rigid quantity-only criteria, and strictly limiting the scope of “relevant national provisions” to exclude departmental rules. These approaches can build a tiered civil-administrative-criminal protection system, uphold criminal modesty, eliminate inconsistent judgments, and balance information security and citizens' legitimate freedom.



References

- 1 Wang P., Zhang J. Conflict and Compromise: A Data Portrait of Judicial Discretion in the Crime of Infringing upon Citizens' Personal Information // Journal of Criminal Investigation Police University of China, 2025. – No. 3. – P. 102.
- 2 Liu X., Wang Z. Adjustment and Reconstruction of Criminal Law Application for the Crime of Infringing upon Citizens' Personal Information // Journal of Anhui University (Philosophy and Social Sciences Edition), 2022. – No. 1. – P. 88.
- 3 Wen L., Tang M. Exploration on the Restrictive Path of the Crime of Infringing upon Citizens' Personal Information Based on Systematic Thinking // Journal of Nanning Normal University (Philosophy and Social Sciences Edition), 2025. – No. 4. – P. 133-134.
- 4 Shi J., Li X. The Dilemma and Solution of the Convergence Between Criminal Law and Administrative Law of the Crime of Infringing Citizen's Personal Information // Jilin University Journal of Humanities and Social Sciences, 2023. – No. 5. – P. 84.
- 5 Chen L. Wenling Investigates the First Case of Infringement on Consumers' Personal Information // Taizhou Daily, 30 March 2021. – P. 4.
- 6 Tan Z., Ran K. On the Articulation Path of Personal Information Protection Mechanism // Social Sciences in Xinjiang, 2023. – No. 2. – P. 108-109.
- 7 Lu Z., Bai Y., Tian J. Selling Public Enterprise Information for Profit: Procuratorate Holds the Actor Not Guilty // Procuratorial Daily, 20 January 2021. – P. 1.
- 8 Roxin C. General Theory of German Criminal Law (Volume 1). Trans. Wang S. – Beijing: Law Press, 2005. – 28 p.
- 9 Li H. Thoughts on the Criminal Law Adjustment of the Crime of Infringing upon Citizens' Personal Information – Against the Background of the Personal Information Protection Law of the People's Republic of China // Journal of CUPL, 2022. – No. 1. – P. 142.
- 10 Sun G. The Dependence and Independence of the Unlawfulness Judgment in Administrative Crime // The Jurist, 2017. – No. 1. – P. 50.
- 11 Zhan Q. The Historical Review and Contemporary Advocacy of Cautious Punishment Idea Originated from the Western Zhou Dynasty and a Comparison with the Foreign Concept of Modesty of Criminal Law // Journal of Social Sciences, 2022. – No. 6. – P. 189.

С. Чжэн¹

¹ Ухань университеті Құқық факультетінің докторанты

(Ухань қ., Қытай Халық Республикасы)

ORCID ID: 0009-0003-3560-6694, e-mail : zxx577374942@gmail.com

СИНГАПУРДАҒЫ ОЙЫН БИЗНЕСІ ТУРАЛЫ ЗАҢНАМАНЫҢ ЕРЕКШЕЛІКТЕРІ: ҚАЗАҚСТАН РЕСПУБЛИКАСЫМЕН САЛЫСТЫРМАЛЫ- ҚҰҚЫҚТЫҚ ТАЛДАУ

Аңдатпа. Мақала қылмыстық және әкімшілік құқық қолданудың кері байланысы жағдайында азаматтардың жеке деректеріне зиян келтіру қылмысының шектелген қолданылуы зерттеледі, осы қылмыстың сотта кең қолданылуының нақты кедергілері талданады, тиісті теориялық және институционалдық негіздер түсіндіріледі және үш мақсатты реттеу жолы ұсынылады. Қытайдың қазіргі қылмыс кодексінде азаматтың жеке мәліметтерін бұзу қылмысының соттық қолданылуы үнемі кеңейіп келеді, бірдей істер бойынша қылмыстық және әкімшілік шараларды қолдануда айырмашылықтар, қылмыстық-әкімшілік нормалардың стандарттары арасындағы қайшылықтар сияқты мәселелер айқын көрінеді. 2025 жылы түзетілген «Әкімшілік тәртіп бұзушылықтар үшін жазалау туралы заң» 56-бабы қылмыстық-әкімшілік кері байланысты қамтамасыз ету және осы қылмыстың қолданылу ауқымын шектеу үшін нормативтік негіз береді. «Мәлішерлік айырмашылық теориясына» сүйене отырып әкімшілік заңбұзушылық пен қылмыстық заңбұзушылықты ажыратамыз, жеңіл қылмыстар дәуіріндегі жазаны сақтықпен қолдану идеясымен бірге осы қылмыс бойынша қылмыстық-әкімшілік кері байланысты жүзеге асырудағы үш негізгі кедергіні жинақтаймыз: нормативтік анықтамалардың бөлшектенуі, қылмыстық және әкімшілік шараларды қолдану тәжірибесінің бір-біріне сәйкес келмеуі, қылмыстық шараны бірінші орынға қою дәстүрінің заңсыздықтан бас тарту мүмкіндігін азайтуы. Қылмыстық-әкімшілік кері байланыс теориясы мен институттық негіздерге сүйене отырып үш жол ұсынамыз: «жеке мәліметтер» ұғымының анықтамасы мен дәрежелік стандарттарды біркелкі ету, «ауыр жағдайларды» нақты мазмұнды негізде анықтау, «мемлекеттің тиісті ережелерін бұзу» ұғымының түсіндірмесін қатаң түрде шектеу.



Түйін сөздер: қылмыстық-әкімшілік байланыс, жеке мәліметтерді қорғау, мәлішерлік айырмашылық теориясы, азаматтың жеке мәліметтерін бұзу қылмысы.

С. Чжэн¹

¹ докторант юридического факультета Уханьского университета
(г. Ухань, Китайская Народная Республика)

ORCID ID : 0009-0003-3560-6694, e-mail: zxx577374942@gmail.com

ОГРАНИЧЕННОЕ ПРИМЕНЕНИЕ ПРЕСТУПЛЕНИЯ «НАРУШЕНИЕ ПРАВА НА ЛИЧНУЮ ИНФОРМАЦИЮ ГРАЖДАН» В УГОЛОВНОМ ПРАВЕ КИТАЯ

Аннотация. В данной статье исследуется ограниченное применение преступления о нарушении неприкосновенности личных данных граждан в условиях обратной координации уголовного и административного правоприменения, анализируются реальные препятствия чрезмерному судебному применению этого преступления, разъясняются соответствующие теоретические и институциональные основы и предлагаются три целенаправленных пути регулирования. В настоящее время судебное применение преступления против персональных данных граждан в уголовном законодательстве Китая постоянно расширяется, обостряются проблемы несоответствия уголовно-административных мер по аналогичным делам и коллизии стандартов уголовно-административных норм. Статья 56 Закона об административных взысканиях за нарушения общественного порядка в редакции 2025 года создает нормативную основу для обратной координации уголовной и административной ответственности и ограничения сферы применения данного преступления. На основе теории количественных различий разграничиваются административные и уголовные правонарушения. С учетом идеи осторожного применения наказаний в эпоху мелких преступлений выявлены три ключевые препятствия обратной координации уголовной и административной ответственности по данному составу преступления: фрагментация нормативных определений, разрыв между практикой применения уголовных и административных мер, а также сужение возможностей освобождения от уголовной ответственности из-за инерции приоритета уголовного преследования. Опираясь на теоретические и институциональные основы обратной координации уголовной и административной ответственности, предлагаются три направления совершенствования: унификация определений и градационных стандартов «персональных данных», содержательная квалификация признака «существенная тяжесть обстоятельств», строго ограничительное толкование понятия «нарушение соответствующих государственных нормативов».

Ключевые слова: координация уголовной и административной ответственности, защита персональных данных, теория количественных различий, преступление против персональных данных граждан.